AFFIDAVIT OF SPECIAL AGENT

I, Michael Willis, being duly sworn, state:

1. I am a special agent with the Federal Bureau of Investigation (FBI) and have been employed as such since April, 1999. During my tenure as an agent, I have investigated white collar, gang, drug, fugitive and violent crimes. In my previous employment, I was a state trooper for more five years during which time I investigated several local violent crime cases that produced numerous convictions. I have also participated in the procurement and execution of numerous search and arrest warrants in a variety of criminal investigations. I am assigned to the Richmond FBI's Central Virginia Violent Crimes Task Force and my duties include investigating bank robberies, armored car robberies, extraterritorial offenses, kidnappings, armed carjacking and theft of government property. The crimes I investigate are violent in nature and usually involve two or more individuals. I am familiar with the methods violent offenders use to conduct their illegal activities, to include, but not limited to their communication methods, use of additional co-conspirators, and reoccurring methods of operation. I have personally participated in the investigation set forth below.

2. This affidavit concerns an investigation by law enforcement into offenses under federal criminal law, specifically: stalking, in violation of 18 U.S.C. § 2261A(2)(A); wire fraud, in violation of 18 U.S.C. § 1343; fraud and related activity in connection with authentication features, in violation of 18 U.S.C. § 1028(a)(7); aggravated identity theft, in violation of 18 U.S.C. § 1028A; and fraud and related activity in connection with computer, in violation of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(7)(B) and 1030(a)(7)(C).

3. Through the course of this investigation, law enforcement agents have established probable cause to believe that Satyasutya Sahas Thumma (hereinafter "THUMMA") committed

the above criminal offenses within the Eastern District of Virginia, and elsewhere within the jurisdiction of the Court, from in or around November 2018 and continuing up through and including March 2019.

4. This affidavit is submitted in support of a search warrant for 1414 West Marshall Street, Apartment #309, Richmond, VA (hereinafter "SUBJECT PREMISES"), and an Apple iPhone X, IMEI 35304309608429 (hereinafter "SUBJECT DEVICE"), wherever that SUBJECT DEVICE may be located, regardless of whether the SUBJECT DEVICE is inside the SUBJECT PREMISES at the time investigators determine the SUBJECT DEVICE's location. The SUBJECT PREMISES and SUBJECT DEVICE to be searched are more particularly described in Attachment A, which is incorporated herein by reference. This affidavit is also submitted in support of a search warrant authorizing the seizure and examination of SUBJECT DEVICE and any other electronic devices found at the SUBJECT PREMISES, and the extraction from the SUBJECT DEVICE and any other seized devices electronically stored information described in Attachment B.

5. This affidavit is based upon information supplied to me by other law enforcement officers, including other special agents employed by the FBI, and local law enforcement personnel who are participating in the investigation. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included each and every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to search the SUBJECT PREMISES and the SUBJECT DEVICE.

RELEVANT STATUTORY PROVISIONS

6. Title 18, United States Code, Section 2261A(2) (stalking), provides in pertinent part that it is illegal when an individual—

> (2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
>
> > (A) places that person in reasonable fear of the death of or serious bodily injury to a person, a pet, a service animal, an emotional support animal, or a horse described in clause (i), (ii), (iii), or (iv) of paragraph (1)(A); or
> >
> > (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A)....

7. Title 18, United States Code, Section 1343 (wire fraud) makes it a crime when:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice....

8. Title 18, United States Code, Section 1028(a)(7) (identity fraud) makes it illegal for whomever to knowingly transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

9. Title 18 United States Code, Section 1028(d)(7) defines "means of identification" as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any— (A) name, social security number, date of birth,

official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number, address, or routing code; or (D) telecommunication identifying information or access device.

10. Title 18, United States Code, Section 1028A(a)(1) (aggravated identity theft), provides in pertinent part that:

> (a)(1) Whoever, during and in relation to felony violation enumerated in subsection(c)[1], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

11. Title 18, United States Code, Sections1030(a)(2)(C), 1030(a)(7)(B) and 1030(a)(7)(C) (fraud and related activity in connection with computers), provide in pertinent part that it is a federal felony offense when an individual:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (C) information from any protected computer; [or]
>
> * * *
>
> (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
>
> * * *
>
> (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization

[1] Included among enumerated offenses in § 1028A(c) are those in Title 18, Chapter 47, including access device fraud under 18 U.S.C. § 1029 and computer fraud under 18 U.S.C. § 1030, as well as those under Title 18, Chapter 63, relating to mail, wire and bank fraud (18 U.S.C. §§ 1341, 1343 and 1344), and conspiracy to commit the same (18 U.S.C. § 1349).

or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

12. Title 18, United States Code, Section 1030(e)(2)(B) defines "protected computer" as a computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state. The Internet is a means or facility of interstate and foreign commerce.

c. Smartphone is a portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary

somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

d. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media, in includes memory incorporated into smartphones.

FACTS AND CIRCUMSTANCES

14. During August 2018, a woman identified herein as "H.R.," started a relationship with THUMMA through the Tinder App. H.R. returned to college in California at the end of summer and continued her relationship with THUMMA through the use of Instagram and FaceTime, during which time she sent THUMMA approximately fifteen nude photos of herself[2]. The relationship with THUMMA continued until November 2018 when H.R. broke it off. THUMMA did not take the breakup well and threatened to post the photographs online and send them to H.R.'s father, who is a Baptist minister.

15. When H.R. returned home from college in November 2018, she met with THUMMA on two separate occasions. The first occasion was at a Tropical Smoothie in Richmond, Virginia, sometime at the end of November 2018, at THUMMA's request to talk

[2] H.R. also sent some of these photos to a second person she met in college named Kevin who she had a brief sexual relationship with. Since the ending of that relationship, H.R. has had little to no contact and no conflict with him.

about the relationship. During this meeting, THUMMA told H.R. he could help her remove the photos off the internet if she spent two weeks with him as a show of kindness for wasting his time in their prior relationship. The second meeting occurred soon after, for which H.R. drove to THUMMA's apartment at 1414 West Marshall Street, Apartment #309 Richmond, VA. When H.R. entered the apartment, THUMMA showed her a website on his Apple MacBook Pro that was already loaded on the screen. H.R. noticed that the website address ended in "**.onion**" rather than ".com" or ".org," and THUMMA typed in her name on the website search bar to show her that none of her nude photos were on the website. H.R. left immediately after.

16. Through my training, experience and discussions with other law enforcement officers, I understand that websites that end in ".onion" are "hidden services" located on the Tor network. Tor is free software for enabling anonymous communication on the Internet. The name Tor is derived from an acronym for the original software project name "The Onion Router." The Tor network is a network of computers, known as "nodes," that are set up to encrypt communication throughout the Tor network. The Tor network encrypts the user's communication in multiple layers of encryption and routes the communication through multiple different machines on the Tor network, each of which strips off one layer of encryption before sending the communication along to the next machine. The Tor network is accessed using a specialized web browser, known as the Tor Browser, and is generally inaccessible using traditional Internet browsers. A Tor "hidden service" is used to serve content to users without the users knowing the true location of the hidden service. This process is facilitated through the encrypted "nodes" and a hidden services directory listing. Tor, the user, and the hidden service expect that any network traffic originated from the user to/from the hidden service will not be

trackable and would not be attributable to the user, therefore creating a sense of privacy and anonymity.

17. On December 25, 2018, an unknown subject texted H.R. on her cellphone from telephone number 772-494-7724, a telephone number that was unfamiliar to H.R., advising her to check her email. Investigators checked the above phone number for carrier information and determined that the number was associated with Pinger with no subscriber information.

Date/Time	From	To	Message
Dec. 25, 2018 1:13 AM	772-494-7724	H.R.	"Email tomorrow 10pm"

18. Pinger is a mobile device application developer for the Sideline mobile application and TextFree mobile application. Both Sideline and TextFree allows a user to send and receive text messages from a mobile device, using a telephone number that is different from their mobile device's telephone number. TextFree and Sideline are available on both the Apple iOS and Google Android application stores. In particular to this investigation, TextFree and Sideline make it possible to use a single mobile device, but make it appear that text messages are being send from another person and/or mobile device by sending and receiving messages using a different telephone number. Pinger also permits sending text messages over the Internet via Wi-Fi connections without having to connect directly to cellular networks.

19. On December 26, 2018, H.R. received the following email from unknown email address GhostFlex@protonmail.com. Approximately four minutes after the email was sent, H.R. received a text message from a second unknown telephone number, 434-338-6149. The phone number was checked for carrier information and it revealed that the number was associated with Pinger with no further subscriber information.

Date/Time	**From**	**To**	**Subject**
Dec. 26, 2018 1:18 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R's name redacted]*** *Nudes*
Message	"i am ghost **[H.R. family residence address redacted]** sence u made that nigga leave we gnna get u and him unless u help us he has 100k in a stock account talk 2 him nd get the password we will help u get it nd u get 10k nd we leave u alone u have until the end of today 2 respond or we get him nd u look below 4 proof"		
Dec. 26, 2018 1:22 PM	*434-338-6149*	*H.R.*	
Message	"Check email"		

20. In addition to the email body message above from GhostFlex@protonmail.com, the email also contained two of the nude photographs of H.R. that H.R. had previously sent to THUMMA. The email also contained the correct street address of H.R.'s family residence, which is located in the Eastern District of Virginia. Your affiant understands this email to indicate that the subject knows where H.R. lives, that "him" is referring to THUMMA, and that H.R. needs to obtain THUMMA's password for THUMMA's stock account containing $100,000. If H.R. does not respond by the end of December 26, 2018, GhostFlex would "get" H.R. and THUMMA.

21. ProtonMail is an email service that provides robust end-to-end encryption between the user and ProtonMail servers, which are located in Switzerland and outside of the jurisdiction of both the United States and European Union. ProtonMail's network architecture is designed around the principle of "zero access." User email stored on ProtonMail's servers is encrypted using an encryption key that ProtonMail does not have access to, thus user email stored on ProtonMail servers is inaccessible to third parties, including law enforcement agencies. ProtonMail can be accessed through a webmail client, the Tor network, or dedicated iOS and Android apps.

22. On December 26, 2018, H.R. received the following email from GhostFlex@protonmail.com. Approximately 13 minutes after the email was sent from GhostFlex@protonmail.com, H.R. received the following text message from telephone number 434-338-6149.

Date/Time	**From**	**To**	**Subject**
Dec. 26, 2018 4:23 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s name redacted].2***
Message	"u rlly r dumb arent u we have corporate from verizon nd att i can see nd hear everything u do even if u change #s ill give u 1 last chance u wont shoot us i am a state officer nd have state officers that work wit me do wht we asked we will see u in church 2nite we in **[H.R.'s hometown redacted]** u have til 12 to let us kno"		
Dec. 26, 2018 4:36 PM	*434-338-6149*	*H.R.*	
Message	"email"		

23. Your affiant understands this message to indicate that the subject has H.R. under surveillance via Verizon Wireless and AT&T, which allows the subject to see and hear everything that H.R. does, even if H.R. changes here telephone number. The subject also claimed to be a "state officer" and has other "state officers" that work with the subject. The subject indicates that he/she was in H.R.'s hometown, and would be at H.R.'s church that evening. H.R.'s church did in fact hold a Wednesday night service on December 26, 2018.

24. On December 26, 2018, H.R. exchanged Apple iMessages with THUMMA, telephone number 540-394-1286, regarding the emails received by H.R. from GhostFlex@protonmail.com. The following messages, in part, were exchanged between H.R. and THUMMA.

Date/Time	**From**	**To**	**Message**
Dec. 26, 2018 7:44 PM	H.R.	THUMMA	"But forreal this is getting very serious. I need to know if this is forreal"
Dec. 26, 2018 7:45 PM	THUMMA	H.R.	"Get help then"

Date/Time	From	To	Message
Dec. 26, 2018 7:45 PM	H.R.	THUMMA	"I went to the police"
Dec. 26, 2018 7:46 PM	THUMMA	H.R.	"Good"
Dec. 26, 2018 7:46 PM	H.R.	THUMMA	'They're suppose to be calling you"
Dec. 26, 2018 7:46 PM	THUMMA	H.R.	"They can call my lawyer if they need to talk to me that bad"
Dec. 26, 2018 7:47 PM	H.R.	THUMMA	'They just want your side dude if you're innocent then they should be able to talk to you"
Dec. 26, 2018 7:49 PM	THUMMA	H.R.	'Last time they wanted to "help" me I ended up getting a felony so I think from past experience I'll give it a hard pass. I told my dad, he told his cop friends, I talked to my lawyer. Got extra security on my phone and computer so I'll be fine without their help"
...	...	...	...
Dec. 26, 2018 8:08 PM	THUMMA	H.R.	"All I did for them is make algorithms like the ones in my account to make money on the stock market. They looked at all my stuff and saw YOU in a picture and asked your name. I didn't go and be like yeah this is **[H.R.'s name redacted]** my ex. Like what. But from what I know most of them are retired marines and officers. I NEVER asked them to do anything to you"
Dec. 26, 2018 8:09 PM	H.R.	THUMMA	"You told me you did'
Dec. 26, 2018 8:09 PM	H.R.	THUMMA	"You said you sent them the pictures of me to send to my dad'
Dec. 26, 2018 8:09 PM	H.R.	THUMMA	'You already told me that"
Dec. 26, 2018 8:12 PM	THUMMA	H.R.	"Never happened, If they truly wanted it they'd get it somehow. Like I said once they talk to my lawyer, they'll be able to check my stuff. They wont find anything of you or anything suspicious"

25. Your affiant understands the messages to indicate that H.R. believed the messages from GhostFlex@protonmail.com and 434-338-6149 to be truthful. THUMMA indicated that there was "extra security on my phone and computer," which may make it more difficult for law

enforcement to access THUMMA's phone and computer without THUMMA's assistance. H.R. also believed that THUMMA already sent nude pictures of H.R. to GhostFlex@protonmail.com and that those pictures were going to be sent to her father.

26. Law enforcement obtained subscriber records from AT&T for telephone number 540-394-1286. Information provided by AT&T indicated that, beginning on August 2, 2014, and continuing through the date of the records on March 18, 2019, the user information associated with telephone number 540-394-1286 was SAHAS THUMMA. AT&T call detail records indicated that the international mobile equipment identity software version (IMEISV) assigned to the phone used by with telephone number 540-394-1286 was 3530430960842907, which is composed of the international mobile equipment identity (IMEI) of was 35304309608429 and software version 07. Based on the IMEI and AT&T's records, the mobile device was an Apple iPhone X phone.

27. On December 30, 2018, H.R. and THUMMA received the following email from GhostFlex@protonmail.com.

Date/Time	**From**	**To**	**Subject**
Dec. 30, 2018 10:20 PM	*GhostFlex@protonmail.com*	*H.R., THUMMA*	***[H.R.'s last name redacted].Thumma.3***
Message	"formula is not workin dnt play around i dnt think ur parents wanna see ur nudes ***[H.R.'s first name redacted]*** im sure ur nudes can go 2 the public 2 i dnt think ur parents wanna see u kidnapped sahas u2 gt until midnite or we come bck"		
Dec. 30, 2018 11:52 PM	*GhostFlex@protonmail.com*	*H.R., THUMMA*	***[H.R.'s last name redacted].Thumma.4***
Message	'psychology of parents mind when they see nudes of their kid stays in their mind forever especially 4 wen it is a daughter goes same 4 wen their kid gets kidnapped looks like we will b back"		

28. Your affiant understands these messages to imply that H.R. may be kidnapped if H.R. and THUMMA do not comply with GhostFlex@protonmail.com's demands.

29. On December 31, 2018, H.R. received the following email and text messages from GhostFlex@protonmail.com and Pinger telephone number 434-338-6149.

Date/Time	**From**	**To**	**Subject**
Dec. 31, 2018 6:01 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s last name redacted].6***
Message	"see how u do now we got sahas go ahead try 2 tlk 2 him you got a month or we kill him lets see wht u do"		
Dec. 31, 2018 6:11 PM	*434-338-6149*	*H.R.*	
Message	"email"		
Dec. 31, 2018 6:20 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s last name redacted].7***
Message	"u have his life in ur hands do we kill him or not answer or he dies"		
Dec. 31, 2018 6:37 PM	*GhostFlex@protonmail.com*	*H.R.*	*dead*
Message	"good luck finding him ***[H.R.'s first name redacted]*** kno 1 of ur exes put a hit on u 2 bad this guy was tlkin 2 u at the time have fun explainin 2 his parents y he died 4 u"		
Dec. 31, 2018 9:32 PM	*GhostFlex@protonmail.com*	*H.R.*	*TimeClock*
Message	"we got him u have 5 min 2 say wht u have to 9:40p we turn it off again if u want to help him say u will cooperate wit us"		
Dec. 31, 2018 9:33 PM	*434-338-6149*	*H.R.*	
Message	"email last warning"		

30. Your affiant understands the above messages as threats of violence against THUMMA if H.R. does not comply with GhostFlex@protonmail.com's demands.

31. Internet Protocol (IP) records obtained from Pinger indicate that on December 31, 2018, at 9:33 PM, Pinger account 434-388-6149, the same account that sent H.R. text messages, was used by IP address **8.30.81.2**. According to open-source records, the network range containing IP address **8.30.81.2** is assigned to Amtech Communications. The investigation determined that **8.30.81.2** is the IP address used to serve Internet access to approximately 60 multi-residential properties in Virginia and other states, including the apartment leased by THUMMA at 1414 West Marshall Street, Apartment 309, Richmond, Virginia.

32. On January 1, 2019, H.R. received the following email and text messages from GhostFlex@protonmail.com and 434-338-6149.

Date/Time	**From**	**To**	**Subject**
Jan. 1, 2019 12:46 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s last name redacted]***
Message	"we gt him in ***[H.R.'s hometown redacted]*** meet us at petersburg VSU 2 let him go if not we will continue torturin him"		
Jan. 1, 2019 11:19 PM	*GhostFlex@protonmail.com*	*H.R.*	*Missing Person Report*
Message	"u see the missing person report that should show u we r serious tell jodi we said hi nd thx 4 gettin snap back we saw u deleted it"		
Jan. 1, 2019 11:31 PM	*434-338-6149*	*H.R.*	
Message	"email he ours"		

33. Your affiant understands "him" to be THUMMA, and that GhostFlex@protonmail.com has taken THUMMA by force, has tortured THUMMA, and will continue to torture THUMMA until H.R. arrives at Virginia State University College of Agriculture, located in Petersburg, Virginia.

34. Internet Protocol (IP) records obtained from Pinger indicate that on January 1, 2019, at 11:30 PM and11:31 PM, Pinger account 434-388-6149 was used by IP address **8.30.81.2**.

35. On January 2 - 3, 2019, H.R. received the following email and text messages from GhostFlex@protonmail.com, 434-338-6149 and THUMMA.

Date/Time	**From**	**To**	**Subject**
Jan. 2, 2019 1:32 PM	*GhostFlex@protonmail.com*	*H.R.*	*last warning*
Message	"come 2 vsu @ 3 nd we will let him go if not we will let him go later nd come 4 someone else close 2 u consider not playin us again wen u see him take. a good look at what we did 2 him"		
Jan. 3, 2019 10:58 AM	*GhostFlex@protonmail.com*	*H.R., THUMMA*	***[H.R.'s last name redacted].Thumma***
Message	"glad we r all free again i think we made it clear if u play us what will happen we will ruin some1s life if it happens agin"		

Date/Time	**From**	**To**	**Subject**
Jan. 3, 2019 12:59 PM	*THUMMA*	*H.R.*	
Message	"I have to talk to you"		
Jan. 3, 2019 1:03 PM	*H.R.*	*THUMMA*	
Message	"What happened?"		
Jan. 3, 2019 9:47 PM	*THUMMA*	*H.R.*	
Message	"I can't really talk yet. My ribs are either fractured or broken. By Monday the doctors said I should be okay to get off my pain meds, so I'll text you then, okay?"		
Jan. 3, 2019 11:07 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s last name redacted].8***
Message	"heard ur talking shit sayin we wont do anything watch that formula is not done yet until it is everyone around u be on watch"		

36. Your affiant understands, from the messages above, that THUMMA was being held by force and suffered physical injury while in captivity by GhostFlex@protonmail.com. THUMMA confirmed that he suffered physical injury in an iMessage to H.R.

37. From January 8 to January 11, 2019, H.R. received the following emails from GhostFlex@protonmail.com and hesh@ctemplar.com.

Date/Time	**From**	**To**	**Subject**
Jan. 8, 2019 12:42 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s name redacted]***
Message	"u see ur boy multiple broken ribs nd surgery our boss will email u soon gl wit him u fuked up now"		
Jan. 9, 2019 2:04 PM	*hesh@ctemplar.com*	*H.R.*	***[H.R.'s first name redacted]***

Date/Time	**From**	**To**	**Subject**
Message	"We just want you to know you fucked up you didnt deliver what we asked & the only person that can help you now is in the hospital and he hates you hoe ass surprised he isnt dead we broke a lot of his ribs and made sure he had internal bleeding if he isnt dead from the surgery ask him so you know we are telling the truth not only do you have ghost people on you now you have us 2 those tinder guys you been talking to they our guys we see your snap story we saw all the messages you got cops around your church and house but that wont save you. You see videos soon of what we did to other people talk to you soon https://www.instagram.com/***[H.R.'s name redacted]***/ https://www.facebook.com/***[H.R.'s name redacted]***/1450535975 ***[H.R.'s relative's name redacted]*** Jodi"		
Jan. 11, 2019 3:35 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s name redacted]***
Message	'u have hesh on u now 2 man has people that can come kill anyl u better start givin us what we want soon"		
Jan. 11, 2019 7:51 PM	*GhostFlex@protonmail.com*	*H.R., hesh@ctemplar.com*	***[H.R.'s name redacted]***
Message	"ur man said u gonna pay us 25k 2 leave u alone send bitcoins to this address XjkdiXsnl2saDa4nhsFsFTw Hesh if this bitch does nt go ahead nd take her we need some1 2 live stream 4 our ppl Ds"		
Jan. 11, 2019 9:10 PM	*GhostFlex@protonmail.com*	*H.R.*	***[H.R.'s name redacted]***
Message	"25k by next week or this will be wht happens hesh will come 4 u 19.jpg, 20.jpg, 26.jpg"		

38. You affiant understands, from the messages above, that "ur boy" referred to THUMMA, and that THUMMA broke numerous rib bones and had surgery to repair the damage. The term "boss" referred to hesh@ctemplar.com, who began sending emails to H.R. during this period. The term "ghost people" referred to people that worked for

hesh@ctemplar.com and who were constantly watching H.R. and knowing H.R.'s whereabouts. It is understood that hesh@ctemplar.com demanded $25,000 in order to be left alone, and payment should be made via BitCoins, a cryptographic currency, to the address XjkdiXsnl2saDa4nhsFsFTw.

39. CTemplar, similar to ProtonMail, is an extremely secure email service. The CTemplar company is headquartered in the Seychelles and has its email servers in Iceland, two countries that both have strong privacy laws. CTemplar uses robust end-to-end encryption for user content, which the company cannot decrypt. CTemplar also does not log IP addresses for its users.

40. The email message on January 11, 2019, at 9:10 PM contained three images attached to the email. The first image depicted a deceased female laying without clothing on her back on what appeared to be a medical examination table. The female appeared to have a yellow tag attached to her right foot. The second image appeared to be a female, without clothing, covered in blood, and held upright by a pole that extended from the ground and through the back of her body and extending through her mouth. The third image appeared to be a female with her hands bounded, body tied to a tree, and lower garments pulled down to her ankles, exposing her rear end. A man, with his head covered by a full-head mask, appeared to be sexually assaulting the female.

41. From January 14 to January 26, 2019, H.R. continued to receive emails from hesh@ctemplar.com and GhostFlex@protonmail.com regarding the non-payment of the $25,000 and how H.R.'s nude photos were going to be distributed.

42. On January 26, 2019, THUMMA sent the following messages, in part, to H.R. via iMessage.

Date/Time	From	To	Message
Jan. 26, 2019 11:55 AM	THUMMA	H.R.	Church girl gonna get exposed, I'll be here watching □□□
Jan. 26, 2019 11:58 AM	THUMMA	H.R.	Plus I'm giving them all your shit today so they can expose you □□□

43. On January 30, 2019 – February 1, 2019, H.R. received the following messages from GhostFlex@protonmail.com.

Date/Time	From	To	Subject
Jan. 30, 2019 11:12 AM	*GhostFlex@protonmail.com*	*H.R.*	*Church*
Message	"now ur church has pics now evrey1 u kno will 2 in the next month c u soon wit 25k or ruin urlife"		
Feb. 1, 2019 10:32 AM	*GhostFlex@protonmail.com*	*H.R., **[H.R.'s family church]**@embarqmail.com*	*Feb1st IMPORTANT MESSAGE*
Message	<no message>		

44. On February 1, 2019, GhostFlex@protonmail.com sent a message to H.R. and [**redacted**]@embarqmail.com, the email address for H.R.'s family church in H.R.'s hometown, containing no text and three nude pictures of H.R.

45. On February 16, 2019, H.R. discovered that her Twitter account, username @[**redacted**], was compromised by an unknown subject. H.R. made the discovery because H.R. was being contacted by friend and family saying that they received nude photos of H.R. via direct message from H.R.'s Twitter account.

46. Law enforcement obtained the logs for H.R.'s Twitter account and determined that on February 16, 2019, at 9:46 AM, IP address **8.30.81.2** was used to log in to H.R.'s Twitter account. On February 16, 2019 at 10:01 AM, the email address for the H.R.'s Twitter account was changed to hesh@ctemplar.com. On February 16, 2019, from 10:05 am through 10:06 AM, ten messages containing nude photos of H.R. were sent from H.R.'s Twitter account to various friends associated with the Twitter account. On February 16, 2019, at 10:09 AM, the IP address

51.15.68.66 was used to log in to H.R.'s Twitter account. Records for the IP address 51.15.68.66 were examined and it was determined that the 51.15.68.66 IP address was a Tor exit node, which is part of the Tor network. In this capacity, Tor was used to hide the true IP address of the subject conducting the malicious activity. Between February 16, 2019, 10:09 AM through 10:25 AM, 19 messages were sent from H.R's Twitter account with 16 containing nude photos of H.R.

47. On February 16 – 23, 2019, H.R. received the following messages from hesh@ctemplar.com and 434-338-6149.

Date/Time	**From**	**To**	**Subject**
Feb. 16, 2019 10:30 AM	*hesh@ctemplar.com*	*H.R.*	*Twitter*
Message	"hahahahahahahhaha more will come if you don't get us that ID"		
Feb. 17, 2019 2:01 AM	*hesh@ctemplar.com*	*H.R.*	*Fb twitter*
Message	"facebook now is ours last chance 4 u 2 try nd get that id"		
Feb. 17, 2019 10:36 AM	*434-338-6149*	*H.R.*	
Message	"U saw wht we can do Last chance 2 get the id picture 4 us"		
Feb. 17, 2019 10:37 AM	*434-338-6149*	*H.R.*	
Message	**"[H.R.'s family residence street address redacted]"**		
Feb. 17, 2019 10:38 AM	*434-338-6149*	*H.R.*	
Message	"U hav until 2morrow 2 get it 4 us Like be4 we will kno if u txted him 2 try"		
Feb. 19, 2019 2:30 AM	*434-338-6149*	*H.R.*	
Message	"We wanted u 2 get ur fb disabled nd u did thx 4 helping us we got ur videos and da ppls names we need 2 send da videos 2"		
Feb. 19, 2019 2:30 AM	*434-338-6149*	*H.R.*	
Message	"Let da games begin"		
Feb. 19, 2019 2:33 AM	*434-338-6149*	*H.R.*	
Message	"ONLY 1 person can stop us Nd u don't talk 2 him Thx 4 da help"		
Feb. 23, 2019 2:13 AM	*434-338-6149*	*H.R.*	
Message	"Ur videos will be out Nd pics Along wit ur parents jobs seeing them Get us that id pic"		

48. You affiant understands that the messages above are referring to a prior request by hesh@ctemplar.com for H.R. to obtain a picture of THUMMA's government identification. On or about February 17, 2019, H.R. discovered that she was unable to access her Facebook account using her telephone number and password. The account was later closed by Facebook.

49. Pinger IP logs revealed that the IP address **8.30.81.2** was used to access the 434-338-6149 Pinger account at the time the text messages were sent on February 19, 2019, at 2:30 AM (2 records) and 2:33 AM.

50. A further review of the 434-338-6149 Pinger account revealed that the account was created on December 26, 2018, and the email address ghostflex@protonmail.com was used to register the account. A review of the IP logs for the 434-338-6149 Pinger account revealed that the **8.30.81.2** IP address was used to access the Pinger account 46 times, beginning on January 1, 2019, and last seen on March 14, 2019.

51. On or about March 8, 2019, a Pen Register/Trap and Trace (PR/TT) order was authorized and installed on the Internet connection for THUMMA's residence at 1414 West Marshall Street, Apartment 309, Richmond, Virginia.

52. Pinger IP records for the 434-338-6149 Pinger account indicated that the **8.30.81.2** IP address access the Pinger account on March 14, 2019, at 5:02 PM. Records from the PR/TT on THUMMA's Internet connection revealed network traffic that originated from THUMMA's Internet connection on March 14, 2019, at 5:02 PM, at the same time the text message was sent from the Pinger account. This indicates that the 434-338-6149 Pinger account is being used by someone that has access to THUMMA's apartment or Internet connection.

53. On March 14, 2019, at approximately 5:04 PM, H.R.'s mother, referred to herein as "R.R.," received the following text message from the 434-338-6149 Pinger account.

Date/Time	From	To	Message
Mar. 14, 2019 5:04 PM	434-338-6149	R.R.	"U destroy my computer we destroy ur name"

54. Pinger IP records for the 434-338-6149 account indicated that the IP address 159.65.233.103 was used in order to send the message to R.R.H.R. on March 14, 2019 at 5:04 PM. A review of the PR/TT records from THUMMA's Internet connection indicated that there was a connection to the same IP address, 159.65.233.103, from THUMMA's Internet connection originating at 5:03 PM and ending. According to open-source records, the IP address 159.65.233.103 belongs to Digital Ocean, an Internet hosting provider. In this particular instance, it appears that the 159.65.233.103 was being used as a proxy server in order to hide that the Pinger account 434-338-6149 was being access from THUMMA's apartment.

55. On March 27, 2019, H.R. and H.R.'s mother R.R. received the following text messages from the 434-338-6149 Pinger account.

Date/Time	From	To	Message
Mar. 26, 2019 6:44 PM	434-338-6149	R.R.	"Since u broke my computer signed "[H.R.'s first name redacted] Nd Becky" ask ur daughter bout her sex tape Nd her FaceTime video Nd ur husband 4 his child pornography"
Mar. 26, 2019 6:45 PM	434-338-6149	H.R.	"U broke my computer ur sex tape is getting out we see u in Richmond"
Mar. 27, 2019 2:55 AM	434-338-6149	H.R.	"Ur next"
Mar. 27, 2019 2:55 AM	434-338-6149	R.R.	"Ur next"

56. Both text messages received by H.R. and R.R. on March 27, 2019, at 2:55 AM also contained a photograph of THUMMA appearing to be in a hospital bed wearing a patient gown containing red marks that appear to be blood. THUMMA's eyes are closed, and his lips and chin appear to have cuts and/or abrasions. Your affiant understands these messages to be a

threat to cause serious bodily injury to H.R. and R.R. A copy of the image sent to H.R. in included as Attachment C, and the image sent to R.R. is included as Attachment D.

57. A review of the PR/TT for THUMMA's Internet connection revealed that there were multiple connections to Pinger IP addresses that were initiated on or about March 26, 2019, at 6:41 PM and March 27, 2019, at 2:54 AM, approximately the same times that the text messages were received by H.R. and R.R. from the 434-338-6149 Pinger account.

58. My investigation has revealed that approximately five hours prior to these two "Ur next" text messages, on March 26, 2019, at around 9:30 p.m., officers with the VCU Police Department responded to the scene of an automobile accident in the 900 block of West Cary Street in Richmond. At the scene officers found sitting THUMMA in the driver's seat of a 2013 Nissan Sentra, VA tag WVY2535, evidently intoxicated. Evidence at the scene suggested that THUMMA's vehicle had struck three parked cars, one of which was struck so hard that it was knocked onto the sidewalk. THUMMA was transported by EMS to the VCU Health Systems Emergency Department. Based on evidence obtained at the scene, as well as a hospital interview with THUMMA, officers charged THUMMA with DUI, case number GT19013612-00. THUMMA has a court date for that DUI on April 24, 2019, at 11:30 a.m., at the Richmond John Marshall General District Court Building.

59. Joseph Seawell, owner of 1414 West Marshall Street apartment #309, Richmond, VA, was interviewed and confirmed that THUMMA is a current tenant of that unit with a lease that expires in June 2019. Seawell also confirmed that the unit has one parking space in the interior parking garage. On March 18, 2019, prior to the March 26 DUI accident discussed above, your affiant conducted a surveillance at 1414 West Marshall Street and observed a blue

Nissan Sentra, VA tag WVY2535, parked in the spot designated for apartment #309. A DMV check of this registration confirmed that it is the registered vehicle for THUMMA.

60. THUMMA's vehicle was heavily damaged, if not totaled, as a result of the March 26, 2019 DUI accident. Because THUMMA stopped driving the Nissan after the accident, and further because his apartment building has restricted access, investigators who had been conducting periodic surveillance of THUMMA's location lost contact with him over the ensuing days. Because of this, on April 5, 2019, I obtained a search warrant, Case No. 3:19-sw-128, to obtain GPS/E-911 location information for THUMMA's iPhone, *i.e.,* the SUBJECT DEVICE. Information obtained from executing that warrant has revealed that from around April 8, 2019, to today's date THUMMA has repeatedly moved locations throughout the Richmond area, and has also made several trips to the area of Winchester, Virginia, where his parents are believed to reside. It is unknown how or in what vehicle THUMMA has been traveling about.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

61. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users, and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

62. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint

scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

63. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Examples of such devices providing a fingerprint unlocking capability are several models of Apple's iPhone, as well as several phones, including but not limited to the Samsung Galaxy, which use the Android operating system. Apple iPhones may be fingerprint unlocked using a function called Touch ID, which during setup allows for registering as many as five (5) fingerprints to unlock the device. Samsung's Galaxy S8 and S8+ models may be configured to be unlocked with as many as four (4) fingerprints. In fact, the number of electronic devices providing a fingerprint unlocking capability, including both smart phones and laptops, is growing continually.

64. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based upon the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

65. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his

or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

66. In my training and experience, users of electronic devices often enable the above-mentioned biometric features because they are considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. In some instances, biometric features are considered a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

67. Related to the above discussion regarding encryption, if a forensic examination is not conducted shortly after seizing the device while it is in an unlocked state, or unlocking the device using biometric features immediately upon seizing it, law enforcement investigators may completely lose the ability to forensically examine the device, assuming the device's owner refuses to disclose the password. The passcode or password that would unlock any such device subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of biometric features necessary to the execution of the search authorized by this warrant.

68. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: 1) more than 48 hours has elapsed since the device was last unlocked; or

2) when the device has not been unlocked using a fingerprint for eight (8) hours *and* the passcode or password has not been entered in the last six (6) days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four (4) hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

69. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of these biometric features, the warrant I am applying for would permit law enforcement personnel to: 1) press or swipe the fingers (including thumbs) of any individual, who is reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s); 2) hold the device(s) in front of the face of those same individuals and activate the facial recognition feature; and/or 3) hold the device(s) in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. In the event that law enforcement is unable to unlock the subject device(s) within the number of attempts permitted by the pertinent operating system, this will simply result in the device(s) requiring the entry of a password or passcode before it can be unlocked.

70. Due to the foregoing, I request that the Court authorize law enforcement personnel to press the fingers (including thumbs) of THUMMA or any other individual who is in possession of the SUBJECT DEVICE, and any other individuals who may be present during the search of the SUBJECT PREMISES, to unlock the SUBJECT DEVICE and any other electronic devices that may be seized at the SUBJECT PREMISES so that investigators may conduct the

search and examination as described in this Affidavit and Attachment B.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

71. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

72. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

73. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

c. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

d. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

e. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on

the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

g. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

h. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, as well as other Internet-facilitated crimes like wire fraud and stalking, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

74. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

75. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

76. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible

that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

77. Based on the information described above, I respectfully submit that there is probable cause to believe, that Satyasutya Sahas Thumma, a.k.a., THUMMA, committed the crimes described in detail above, and that evidence of those crimes may be found at the 1414 West Marshall Street, Apartment #309, Richmond, VA 23224, the SUBJECT PREMISES, and on the Apple iPhone X IMEI 35304309608429, the SUBJECT DEVICE. Accordingly, I respectfully request that a search warrant be issued for the SUBJECT PREMISES and the SUBJECT DEVICE.

78. Further, because of the circumstances discussed in paragraph 60 above regarding THUMMA's unknown mode of transportation and recent lack of consistent residence, I respectfully request that agents executing this warrant be authorized to seize the SUBJECT DEVICE wherever it may be located, regardless of whether the SUBJECT DEVICE is inside the SUBJECT PREMISES, including from THUMMA's person, and/or any vehicle that agents have probable cause to believe that THUMMA has stored the SUBJECT DEVICE therein.

Respectfully submitted,

Michael Willis
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me this date: April 19, 2019

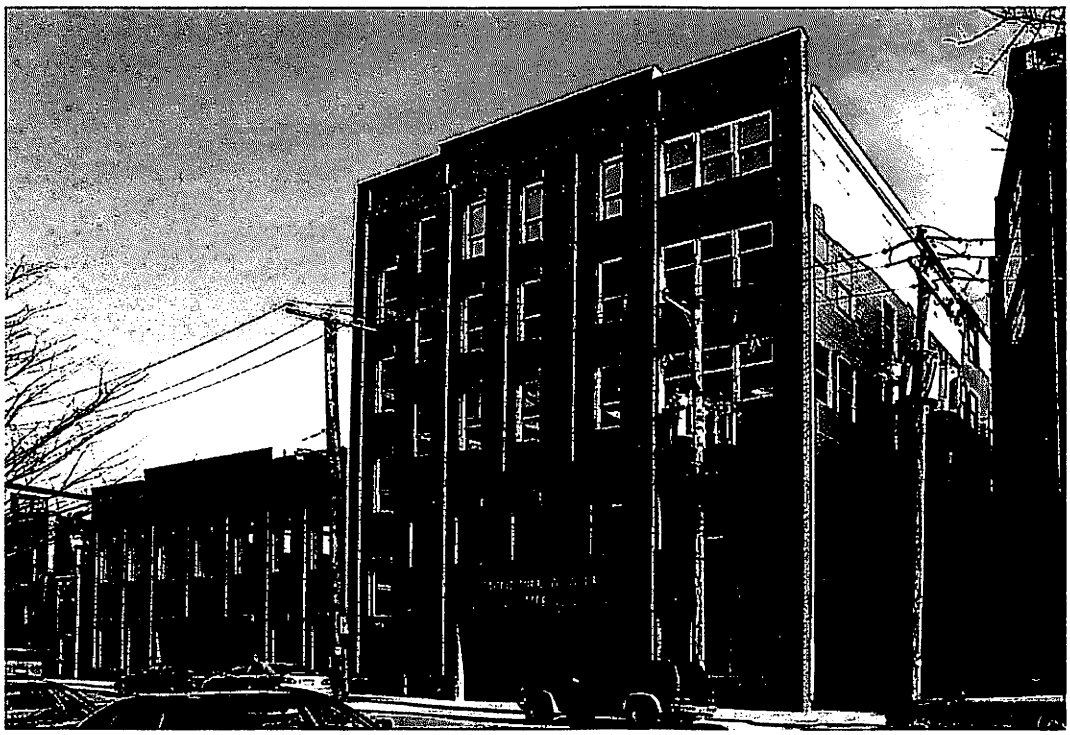
/s/
David J. Novak
United States Magistrate Judge

ATTACHMENT A

Places to Be Searched

SUBJECT PREMISES

The location to be searched is 1414 West Marshall Street, Apartment #309, Richmond, VA. It is an Apartment building. The residence is pictured below:



SUBJECT DEVICE

An Apple iPhone X, IMEI 35304309608429. Agents executing this warrant are authorized to seize the SUBJECT DEVICE wherever it may be located, regardless of whether the SUBJECT DEVICE is inside the SUBJECT PREMISES, including from the person of Satyasutya Sahas Thumma, a.k.a., "THUMMA," and/or any vehicle that agents have probable cause to believe that therein THUMMA has stored the SUBJECT DEVICE.

ATTACHMENT B

Property to be Seized

1. All records relating to violations of Title 18 U.S.C. §§ 2261A, 1343, 1028, and 1030(a)(2)(C) and 1030(a)(7)(B), those violations involving SATYASUTYA SAHAS THUMMA and occurring after September 1, 2018, and continuing to the date of this affidavit and warrant, including:

a. Records and information relating to the stalking of H.R. and R.R.;

b. Records and information relating to the possession and transmission of nude photographs of H.R.;

c. Records and information relating to the Facebook and Twitter accounts belonging to H.R.;

d. Records and information relating to a conspiracy to defraud H.R. and R.R.;

e. Records and information relating to an access of Facebook and Twitter accounts belonging to H.R. and R.R.;

f. Records and information relating to H.R. and R.R.;

g. Records and information relating to the email accounts ghostflex@protonmail.com and hesh@ctemplar.com;

h. Records and information relating to the Pinger accounts 772-494-7724 and 434-338-6149;

i. Records and information relating to THUMMA's telephone number 540-394-1286;

j. Records and information relating to the identity or location of the THUMMA;

k. Records and information relating to the Internet connection originating from THUMMA's residence.

l. Records evidencing the use of Internet Protocol addresses 8.30.81.2, 51.15.68.66, 159.65.233.103, and any other IP addresses used to communicate with H.R., R.R., their family members and their family church, including:

i. records of Internet Protocol addresses used;

ii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Computers or storage media used as a means to commit the violations described above, including unauthorized access to a protected computer in violation of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(7)(B) and 1030(a)(7)(C).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware, including but not limited to the SUBJECT DEVICE.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the SUBJECT DEVICE and any other COMPUTER seized during the search of the SUBJECT PREMISES described in Attachment A, regarding the SUBJECT DEVICE and other COMPUTERS law enforcement personnel are authorized to: 1) press or swipe the fingers (including thumbs) of any individual, who is reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device(s); 2) hold the device(s) in front of the face those same individuals and activate the facial recognition feature; and/or 3) hold the device(s) in front of the face of those same individuals and activate the iris

recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

Verizon LTE 8:34 AM 100%

(434) 338-... Sahas

come see me, i don't care about H.R.'s first name redacted **past mistakes doesn't affect me**

Today 2:55 AM

(434) 338-6149

Ur next

Verizon LTE 10:43 AM 63%

Touch to return to call 02:51

73

(434) 338-6149 >

Wednesday 2:55 AM

Ur next